KING & SPALDING

King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
Tel: +1 212 556 2100
Fax: +1 212 556 2222
www.kslaw.com

Laura Harris
Partner
Direct Dial: +1 212 790 5360
Direct Fax: +1 212 556 2222
lharris@kslaw.com

January 31, 2022

BY ECF

The Honorable Denise L. Cote
United States District Judge
Southern District of New York
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street
New York, New York 10007

Re: *Google LLC v. Starovikov et al.*, 1:21-cv-10260-DLC

Dear Judge Cote:

I write on behalf of Google LLC ("Google") in the above-referenced action to provide a status update on Google's efforts to disrupt the Glupteba botnet, pursuant to the Preliminary Injunction entered December 16, 2021. *See* ECF 17 at 15.

Google's disruption efforts pursuant to the Temporary Restraining Order and Preliminary Injunction Order have impaired the Glupteba botnet and the operations of the criminal enterprise that supports it (the "Enterprise"). As a result of these efforts, nearly 100 domains and IP addresses have been suspended or otherwise disabled, frustrating the Enterprise's distribution of malware, its use of command-and-control servers ("C2 servers") to communicate with infected devices, and its operation of storefronts to effectuate its criminal schemes. At least one of the Enterprise's prominent storefronts, Dont.farm, has folded its operations altogether. As anticipated, the Enterprise has attempted to circumvent these disruptions by exploiting the blockchain to direct infected devices to new domains. Google has worked to identify these new domains and has succeeded in having them suspended as well.

This letter summarizes Google's efforts to disrupt the botnet and the Enterprise that runs it. Google also proposes a schedule for its motion for default judgment and permanent injunction.

Background and Procedural History[1]

Glupteba is a botnet—a network of internet-connected devices, each of which is infected by malware. Over the past decade, this malware has silently infiltrated more than a million computers and other devices around the globe for illicit purposes, including:

- **Stolen Accounts**. Stealing personal login information (for Google and other accounts) from infected devices to sell access to those accounts.
- **Credit Card Fraud**. Selling credit cards for fraudulent purchases of ads or services from Google and other web-based companies.
- **Disruptive Advertising**. Selling the placement of disruptive ads (e.g., pop-up ads in videos) on infected devices.
- **Proxying**. Selling access to victims' infected devices to relay, or "proxy," communications to conceal the location of bad actors.
- **Cryptojacking**. Hijacking the computing power of infected devices to generate cryptocurrency.

In December 2021, Google filed its Complaint in this case against Dmitry Starovikov, Alexander Filippov, and Does 1 through 15, asserting claims based on the Racketeer Influenced and Corrupt Organizations Act (RICO), the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Lanham Act, tortious interference of business relationships, and unjust enrichment. *See* ECF 4. Google also moved for a temporary restraining order, seeking authority to disrupt the botnet by requiring domain registrars, server hosts, and other entities to suspend or otherwise disable components of the operations of the botnet and the Enterprise. Those domains and IP addresses were identified in Appendix A to the Complaint. *See* ECF 5-1.

On December 2, 2021, this Court granted Google's temporary restraining order. ECF 8 (the "Temporary Restraining Order"). As described in more detail below, Google served the order on relevant entities in order to disrupt the servers and domains identified in Appendix A. The vast majority of those served with the Temporary Restraining Order promptly complied with the order's requirements.

[1] More detail can be found in the Complaint (ECF 5), Google's request for a temporary restraining order (ECF 19), and the Huntley Declaration (ECF 21).

The Enterprise has responded by trying to reconstitute the botnet using new domains and new servers. On December 16, this Court issued a preliminary injunction expanding the scope of the injunction beyond the list in Appendix A. ECF 17 (the "Preliminary Injunction Order"). That order permitted Google to serve the order on any entities providing services relating to the domains and IP addresses identified by Google as connected to the Enterprise. *Id.* at 12.

Defendants Dmitry Starovikov and Alexander Filippov have not entered an appearance, filed an answer, or otherwise participated in this litigation to defend themselves.

Google's Disruption of the Botnet

Google's disruption efforts have proceeded on several different fronts. To date, Google has shut down 97 domains and IP addresses associated with Glupteba pursuant to the Temporary Restraining Order and Preliminary Injunction Order.

Disrupting the C2 Servers. The Enterprise uses C2 servers to provide instructions to the devices comprising the botnet to perform disruptive or criminal tasks. Without the C2 servers, the botnet cannot receive new instructions.

Google identified seven IP addresses associated with C2 servers for the Glupteba botnet in Appendix A to its Complaint. As a result of Google's disruption efforts, all seven C2 servers originally identified in Appendix A are no longer operating.

Since that initial disruption, the Enterprise has established new C2 servers, and Google has continued to serve the Preliminary Injunction Order on registrars that maintain domains associated with the new C2 servers. As a result of those efforts, five new domains used to route communications between the new C2 servers and the botnet have been suspended.

Disrupting Storefronts and Recruiting Sites. As discussed above, the Enterprise uses the Glupteba malware to steal login credentials for Google and other accounts. It also uses various storefronts to sell access to the stolen accounts and proxies, and even recruit developers. Pursuant to the Temporary Restraining Order and Preliminary Injunction Order, Google has disrupted numerous domains associated with these activities, including Dont.farm, Extracard.net, and AWMProxy.net.

Since the initial shutdowns, the Enterprise has attempted to create new domains for certain of these purposes. Google has served the Preliminary Injunction Order on the relevant domain registrars, resulting in additional suspensions.

To date, 15 domains associated with storefronts or recruiting have been shut down pursuant to this Court's orders.

Disrupting Other Botnet Operations. Other aspects of the Glupteba botnet's operations also require the use of servers. For example, the botnet uses "content delivery network" servers to download new modules to infected devices. These new modules update the malware, and arm the botnet with the ability to perform new types of illicit activities. Additionally, to infect new devices, the Enterprise uses websites to deliver the malware to unsuspecting victims via "droppers." In other words, the websites trick a user to click on a link, resulting in the download and installation of the malware on their device. Google has disrupted 57 domains associated with content delivery network servers, droppers, and other Enterprise operations.

Suspending Google Accounts Associated With The Enterprise. Since initiating this litigation, Google has suspended more than 130 Google accounts associated with individuals and entities behind the Enterprise. This was on top of the numerous platform-based actions that Google had taken over the past year, including terminating approximately 63 million Google Docs, 1,183 Google accounts, 908 Cloud Projects, and 870 Google Ads accounts associated with the distribution of Glupteba malware.

Proposed Schedule

Google proposes the following schedule for its request for entry of default and motion for default judgment and a permanent injunction:

February 7, 2022	Request for entry of default under Rule 55(a)
21 Days After Any Entry Of Default	Motion for default judgment under Rule 55(b) and permanent injunction

A proposed scheduling order is attached as **Exhibit A.**

Respectfully submitted,

/s/ Laura Harris

Laura Harris